

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-321748

(43)Date of publication of application : 12.12.1997

(51)Int.Cl.

H04L 9/08

G09C 1/00

G09C 1/00

(21)Application number : 08-154991

(71)Applicant : TRANS KOSUMOSU KK

(22)Date of filing : 27.05.1996

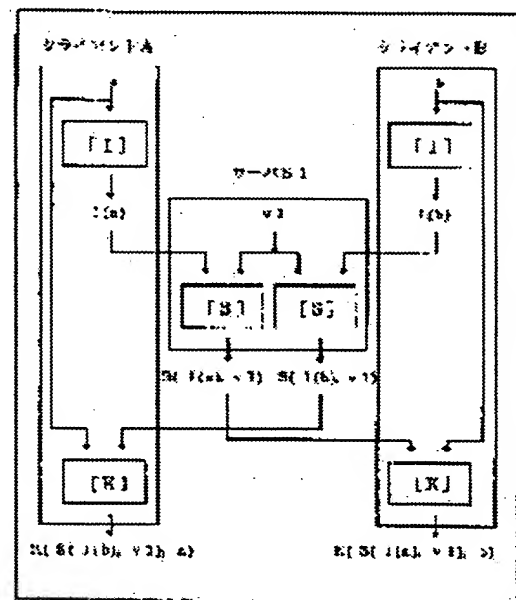
(72)Inventor : OKUDA MASATAKA  
ISHIOKA HIDEAKI

(54) COMMUNICATION SYSTEM BY SHARED CRYPTOGRAPHIC KEY, SERVER DEVICE AND CLIENT DEVICE FOR THE SYSTEM, AND METHOD FOR SHARING CRYPTOGRAPHIC KEY IN COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To enable the operation of a system for changing a cryptographic key to be shared at a short time interval and to rapidly improve the stability of the cryptographic system by changing the shared cryptographic key only by means of the change of a control variable in a server while a password at a client side is fixed.

SOLUTION: A client A generates specific  $I(a)$  through the use of a specific  $I$  generating algorithm ( $I$ ) and informs it to the server  $S1$ . The server  $S1$  generates the open  $idS(I(b), v1)$  of the client B through the use of an open  $S$  generating algorithm ( $S$ ) with the control variable  $v1$  which is secretly managed by the server  $S1$  as an input and reports it to the client A. The client A generates the cryptographic key  $K(S(I(b), v1), a)$  through the use of a cryptographic key generating algorithm ( $K$ ) with the open  $S(I(b), v1)$  of the client B and the self secret password ( $a$ ) as the input.



## LEGAL STATUS

[Date of request for examination] 04.06.1998

[Date of sending the examiner's decision of rejection] 27.12.2001

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-321748

(43) 公開日 平成9年(1997)12月12日

(51) Int.Cl. <sup>8</sup>	識別記号	序内整理番号	F I	技術表示箇所
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 D
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 D
		7259-5 J		6 3 0 E
	6 6 0	7259-5 J		6 6 0 E
			H 0 4 L 9/00	6 0 1 E

審査請求 未請求 請求項の数9 F D (全 13 頁)

(21) 出願番号 特願平8-154991

(22) 出願日 平成8年(1996)5月27日

(71) 出願人 396011831

トランス・コスモス株式会社  
東京都港区赤坂3丁目3番3号

(72) 発明者 奥田 昌孝

東京都渋谷区猿樂町17-16 代官山フォーラム301

(72) 発明者 石岡 英明

千葉県市川市柏井町1-1229-41

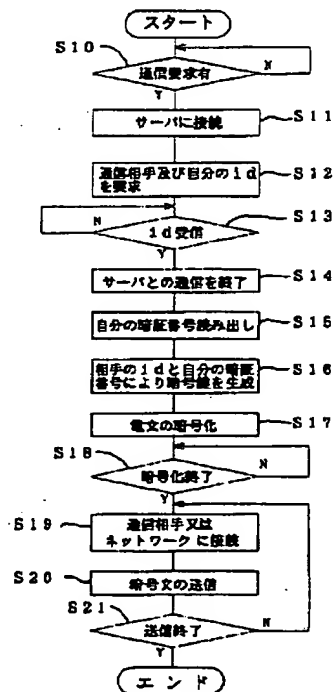
(74) 代理人 弁理士 二瓶 正敬

(54) 【発明の名称】 共有暗号鍵による通信システム、同システム用サーバ装置、同システム用クライアント装置、及び通信システムにおける暗号鍵の共有方法

(57) 【要約】

【課題】 不特定多数との暗号通信に適して、全エンティティが共通の鍵を共有することが可能で、また、安全のため公開情報を変える場合、自分の秘密情報を変更する必要がある共有暗号鍵による通信システムを提供する。

【解決手段】 クライアント (A、B) 側の暗証番号は一定のまま、サーバ (S1) の制御変数  $v$  1 の変更のみで共有する暗号鍵  $K$  を変更できるようにしている。このため、短い時間間隔で、共有する暗号鍵を変化させるシステム運用が可能となり、暗号システムの安全性が飛躍的に向上する。また、サーバの制御変数にある特定の値に設定することでサーバ所属のクライアントグループ内で同じ暗号鍵を共有できるようにしている。このため、緊急時など、特別な状況においてサーバの制御のみでグループ内の暗号化を解除することができる



## 【特許請求の範囲】

【請求項 1】 少なくともクライアント A、クライアント B、サーバ S1 により構成される共有暗号鍵による通信システムであって、

前記クライアント A は、予め定めた自分の暗証番号 a 及び固有 id 生成アルゴリズム [I]、並びに暗号鍵生成アルゴリズム [K] を保持する記憶手段と、前記暗証番号 a 及び固有 id 生成アルゴリズム [I] を用いて固有 id I (a) を生成する手段と、生成された固有 id I (a) を前記サーバ S1 へ通知する手段と、前記クライアント B との共通鍵を生成するために、前記サーバ S1 へ前記クライアント B の公開 id を要求する手段と、前記サーバ S1 から送信される前記クライアント B の公開 id S (I (b), v1) と前記暗証番号 a を入力として前記暗号鍵生成アルゴリズム [K] を用いて暗号鍵 K (S (I (b), v1), a) を生成する手段とを有し、

前記クライアント B は、予め定めた自分の暗証番号 b 及び固有 id 生成アルゴリズム [I]、並びに暗号鍵生成アルゴリズム [K] を保持する記憶手段と、前記暗証番号 b 及び固有 id 生成アルゴリズム [I] を用いて固有 id I (b) を生成する手段と、生成された固有 id I (b) を前記サーバ S1 へ通知する手段と、前記サーバ S1 又は前記クライアント A 及びクライアント B が接続されたネットワーク経由で前記クライアント A の公開 id を入手し、前記クライアント A の公開 id S (I (a), v1) と前記暗証番号 b を入力として前記暗号鍵生成アルゴリズム [K] を用いて暗号鍵 K (S (I (a), v1), b) を生成する手段とを有し、

前記サーバ S1 は制御変数 v1 を生成する手段と、前記クライアント A から通知された固有 id I (a) 及び前記クライアント B から通知された固有 id I (b) を保持するとともに、秘密で管理する前記制御変数 v1 並びに公開 id 生成アルゴリズム [S] を保持する記憶手段と、前記クライアント A からの要求を受けたときは、前記クライアント B の固有 id I (b) と前記制御変数 v1 と、前記公開 id 生成アルゴリズム [S] を用いて前記クライアント B の公開 id S (I (b), v1) を生成する手段と、生成された前記クライアント B の公開 id S (I (b), v1) を前記クライアント A に送信する手段と、前記クライアント A の固有 id I (a) と前記制御変数 v1、前記公開 id 生成アルゴリズム [S] を用いて前記クライアント A の前記公開 id S (I (a), v1) を生成する手段と、生成された前記公開 id S (I (a), v1) を前記クライアント A に送信する手段とを有し、

前記アルゴリズム [I]、[S]、[K] が  $K(S(I(b), v1), a) = K(S(I(a), v1), b)$  を満足するものである共有暗号鍵による通信システム。

【請求項 2】 前記サーバ装置が制御変数 v1 を生成する手段と、前記クライアント A から通知された固有 id I (a) 及び前記クライアント B から通知された固有 id I (b) を保持するとともに、秘密で管理する前記制御変数 v1 並びに公開 id 生成アルゴリズム [S] を保持する記憶手段と、前記クライアント A からの要求を受けたときは、前記クライアント B の固有 id I (b) と前記制御変数 v1 と、前記公開 id 生成アルゴリズム [S] を用いて前記クライアント B の公開 id S (I (b), v1) を生成する手段と、生成された前記クライアント B の公開 id S (I (b), v1) を前記クライアント A に送信する手段と、前記クライアント A の固有 id I (a) と前記制御変数 v1、前記公開 id 生成アルゴリズム [S] を用いて前記クライアント A の前記公開 id S (I (a), v1) を生成する手段と、生成された前記公開 id S (I (a), v1) を前記クライアント A に送信する手段とを有するものである請求項 1 記載の共有暗号鍵による通信システム用サーバ装置。

【請求項 3】 前記クライアント装置が予め定めた自分の暗証番号 a 及び固有 id 生成アルゴリズム [I]、並びに暗号鍵生成アルゴリズム [K] を保持する記憶手段と、前記暗証番号 a 及び固有 id 生成アルゴリズム [I] を用いて固有 id I (a) を生成する手段と、生成された固有 id I (a) を前記サーバ S1 へ通知する手段と、前記クライアント B との共通鍵を生成するために、前記サーバ S1 へ前記クライアント B の公開 id を要求する手段と、前記サーバ S1 から送信される前記クライアント B の公開 id S (I (b), v1) と前記暗証番号 a を入力として前記暗号鍵生成アルゴリズム [K] を用いて暗号鍵 K (S (I (b), v1), a) を生成する手段とを有する請求項 1 記載の通信システム用クライアント装置。

【請求項 4】 少なくともクライアント A、クライアント B、サーバ S1 により構成される通信システムにおける暗号鍵の共有方法であって、

前記クライアント A が、前もって自分の暗証番号 a を定め、固有 id 生成アルゴリズム [I] を用いて固有 id I (a) を生成するステップと、

生成された固有 id I (a) を前記サーバ S1 へ通知するステップと、

前記クライアント B が、前もって自分の暗証番号 b を定め、固有 id 生成アルゴリズム [I] を用いて固有 id I (b) を生成するステップと、

生成された固有 id I (a) を前記サーバ S1 へ通知するステップと、

前記クライアント A が、前記クライアント B との共通鍵を生成するために、前記サーバ S1 へ前記クライアント B の公開 id を要求するステップと、

前記サーバ S1 が前記クライアント A からの要求を受

け、保有している前記クライアントBの固有id I (b)と前記サーバが秘密で管理している制御変数v1を入力として、公開id生成アルゴリズム[S]を用いて前記クライアントBの公開id S(I (b), v1)を生成するステップと、

生成された前記クライアントBの公開id S(I (b), v1)を前記クライアントAに送信するステップと、

前記サーバS1が、保有している前記クライアントAの固有id I (a)とv1から前記クライアントAの公開id S(I (a), v1)を生成するステップと、生成された前記クライアントAの公開id S(I (a), v1)を前記クライアントAに送信するステップと、

前記クライアントAが入手した前記クライアントBの公開id S(I (b), v1)と前記暗証番号aを入力として暗号鍵生成アルゴリズム[K]を用いて暗号鍵 K(S(I (b), v1), a)を生成するステップと、

前記クライアントBが前記サーバS1又は前記クライアントA及び前記クライアントBの接続されたネットワーク経由で前記クライアントAの公開idを入手し、暗号鍵 K(S(I (a), v1), b)を生成するステップとを、

有し、

前記アルゴリズム[I]、[S]、[K]が $K(S(I (b), v1), a) = K(S(I (a), v1), b)$ を満足するものである通信システムにおける暗号鍵の共有方法。

【請求項5】 少なくともサーバS1に管理されるクライアントA、サーバS2に管理されるクライアントC、前記サーバS1と前記サーバS2を管理する親サーバS3により構成される共有暗号鍵による通信システムであって、

前記クライアントAは、予め定めた自分の暗証番号a及び固有id生成アルゴリズム[I]、並びに暗号鍵生成アルゴリズム[K]を保持する記憶手段と、前記暗証番号a及び前記固有id生成アルゴリズム[I]を用いて固有id I (a)を生成する手段と、生成された固有id I (a)を前記サーバS1へ通知する手段と、前記クライアントCとの共通鍵を生成するために、前記サーバS1へ前記クライアントCの公開idを要求する手段と、前記サーバS1から送信される前記クライアントCの3次公開id S(S(S(I (c), v2), v3), v1)と前記暗証番号aを入力として前記暗号鍵生成アルゴリズム[K]を用いて暗号鍵 K(S(S(S(I (c), v2), v3), v1), a)を生成する手段とを有し、

前記クライアントCは、予め定めた自分の暗証番号c及び固有id生成アルゴリズム[I]、並びに暗号鍵生成

アルゴリズム[K]を保持する記憶手段と、前記暗証番号c及び固有id生成アルゴリズム[I]を用いて固有id I (c)を生成する手段と、生成された固有id I (c)を前記サーバS2へ通知する手段と、前記クライアントA及びクライアントCが接続されたネットワーク経由で前記クライアントAの3次公開id S(S(S(I (a), v1), v3), v2)を入手し、前記クライアントAの前記3次公開id S(S(S(I (a), v1), v3), v2)と前記暗証番号cを入力として前記暗号鍵生成アルゴリズム[K]を用いて暗号鍵 K(S(S(S(I (a), v1), v3), v2), c)を生成する手段とを有し、

前記サーバS1は前記クライアントAから通知された固有id I (a)を保持するとともに、秘密で管理する制御変数v1並びに公開id生成アルゴリズム[S]を保持する記憶手段と、前記クライアントAからの要求を受けたときは、要求相手が自グループに属するか否かを判断する手段と、自グループに属さない要求相手のときは前記親サーバS3に前記クライアントAからの要求を転送する手段と、前記親サーバS3から受信した前記クライアントCの2次公開id S(S(I (c), v2), v3)と、前記制御変数v1と、前記公開id生成アルゴリズム[S]から前記3次公開id S(S(S(I (c), v2), v3), v1)を生成して前記クライアントAに送信する手段とを有し、

前記サーバS2は前記クライアントCから通知された固有id I (c)を保持するとともに、秘密で管理する制御変数v2並びに公開id生成アルゴリズム[S]を保持する記憶手段と、前記親サーバS3からの要求を受けたときは、前記クライアントCの固有id I (c)と前記制御変数v2と、前記公開id生成アルゴリズム[S]を用いて前記クライアントCの1次公開id S(I (c), v2)を生成する手段と、生成された前記クライアントCの1次公開id S(I (c), v2)を前記親サーバS3に送信する手段とを有し、

前記親サーバS3は前記サーバS2から送信された前記クライアントCの1次公開id S(I (c), v2)を保持するとともに、秘密で管理する制御変数v3並びに公開id生成アルゴリズム[S]を保持する記憶手段と、前記サーバS1からの要求を前記サーバS2に転送する手段と、前記サーバS2から前記クライアントCの1次公開id S(I (c), v2)を受けたときは、前記制御変数v3と、前記公開id生成アルゴリズム[S]を用いて前記クライアントCの前記2次公開id S(S(I (c), v2), v3)を生成する手段と、生成された前記クライアントCの2次公開id S(S(I (c), v2), v3)を前記サーバS1に送信する手段とを有し、

前記アルゴリズム[I]、[S]、[K]が $K(S(S(S(I (c), v2), v3), v1), a) = K$

(S (S (S (I (a), v1), v3), v2), c) を満足するものである共有暗号鍵による通信システム。

【請求項6】 前記サーバS1が、前記クライアントAから通知された固有id I (a) を保持するとともに、秘密で管理する制御変数v1並びに公開id生成アルゴリズム[S]を保持する記憶手段と、前記クライアントAからの要求を受けたときは、要求相手が自グループに属するか否かを判断する手段と、自グループに属さない要求相手のときは前記親サーバS3に前記クライアントAからの要求を転送する手段と、前記親サーバS3から受信した前記クライアントCの2次公開id S (S (I (c), v2), v3) と、前記制御変数v1と、前記公開id生成アルゴリズム[S]から前記3次公開id S (S (S (I (c), v2), v3), v1) を生成して前記クライアントAに送信する手段とを有する請求項5記載の通信システム用サーバ装置。

【請求項7】 前記親サーバS3が、前記サーバS2から送信された前記クライアントCの1次公開id S (I (c), v2) を保持するとともに、秘密で管理する制御変数v3並びに公開id生成アルゴリズム[S]を保持する記憶手段と、前記サーバS1からの要求を前記サーバS2に転送する手段と、前記サーバS2から前記クライアントCの1次公開id S (I (c), v2) を受けたときは、前記制御変数v3と、前記公開id生成アルゴリズム[S]を用いて前記クライアントCの前記2次公開id S (S (I (c), v2), v3) を生成する手段と、生成された前記クライアントCの2次公開id S (S (I (c), v2), v3) を前記サーバS1に送信する手段とを有する請求項5記載の通信システム用サーバ装置。

【請求項8】 前記クライアント装置が、予め定めた自分の暗証番号a及び固有id生成アルゴリズム[I]、並びに暗号鍵生成アルゴリズム[K]を保持する記憶手段と、前記暗証番号a及び固有id生成アルゴリズム[I]を用いて固有id I (a) を生成する手段と、生成された固有id I (a) を前記サーバS1へ通知する手段と、前記クライアントCとの共通鍵を生成するために、前記サーバS1へ前記クライアントCの公開idを要求する手段と、前記サーバS1から送信される前記クライアントCの3次公開id S (S (S (I (c), v2), v3), v1) と前記暗証番号aを入力として前記暗号鍵生成アルゴリズム[K]を用いて暗号鍵 K (S (S (S (I (c), v2), v3), v1), a) を生成する手段とを有する請求項5記載の通信システム用クライアント装置。

【請求項9】 少なくともサーバS1に管理されるクライアントA、サーバS2に管理されるクライアントC、前記サーバS1と前記サーバS2を管理する親サーバS3により構成される通信システムにおける暗号鍵の共有

方法であって、

前記クライアントAが、前もって自分の暗証番号aを定め、固有id生成アルゴリズム[I]を用いて固有id I (a) を生成するステップと、

生成された固有id I (a) を前記サーバS1へ通知するステップと、

前記クライアントCが、前もって自分の暗証番号cを定め、固有id生成アルゴリズム[I]を用いて固有id I (c) を生成するステップと、

生成された固有id I (a) を前記サーバS2へ通知するステップと、

前記クライアントAが、前記クライアントCとの共通鍵を生成するために、前記サーバS1へ前記クライアントCの公開idを要求するステップと、

要求された通信相手である前記クライアントCが自グループに属するか否かを前記サーバS1が判断するステップと、

前記クライアントCが自グループに属しないときは、前記サーバS1が前記親サーバS3へ前記クライアントCの公開idを要求するステップと、

前記親サーバS3が、前記サーバS1から要求された前記クライアントCを管理するサーバS2へCの公開idを要求するステップと、

前記サーバS2が、保有している前記クライアントCの固有id I (c) と自らの制御変数v2を入力としてアルゴリズム[S]を用いて、前記クライアントCの1次公開id S (I (c), v2) を生成するステップと、

前記サーバS2が、生成された前記1次公開idを前記親サーバS3へ送信するステップと、

前記親サーバS3が、前記1次公開id S (I (c), v2) と自らの制御変数v3を入力としてアルゴリズム[S]を用いて、2次公開id S (S (I (c), v2), v3) を生成するステップと、

前記親サーバS3が生成された前記2次公開id S (S (I (c), v2), v3) を前記サーバS1へ送信するステップと、

前記サーバS1が前記2次公開id S (S (I (c), v2), v3) と前記制御変数v1と前記アルゴリズム[S]を用いて、3次公開id S (S (S (I (c), v2), v3), v1) を生成するステップと、

前記サーバS1が、生成された前記3次公開id S (S (S (I (c), v2), v3), v1) を前記クライアントAへ送信するステップと、

前記クライアントAが前記3次公開id S (S (S (I (c), v2), v3), v1) と前記暗証番号aとアルゴリズム[K]を用いて暗号鍵 K (S (S (S (I (c), v2), v3), v1), a) を生成するステップと、

前記クライアントCが前記暗証番号cとアルゴリズム[K]を用いて暗号鍵 $K(S(S(S(I(a), v1), v3), v2), c)$ を生成するステップとを有し、

前記アルゴリズム[I]、[S]、[K]が $K(S(S(S(I(c), v2), v3), v1), a) = K(S(S(S(I(a), v1), v3), v2), c)$ を満足するものである通信システムにおける暗号鍵の共有方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信システムにおける暗号通信に関し、特に有線、無線のコンピュータネットワーク、移動体通信システムなどにおける通信文の暗号化とその復号における暗号鍵の共有方法の改良に関する。

【0002】

【従来の技術】

【表1】従来から各種の暗号鍵の共有方法があるが、これらの概略は次のとおりである（図7～9参照）。

<第1の方法>各エンティティが想定される全ての通信相手と個別に暗号鍵を共有する方法。

<第2の方法>各エンティティが自分の秘密情報に基づき公開情報を作成し、これを読み出し自由であるが書き込みや消去は厳密に管理された公開ファイルに登録し、通信の際に自分の秘密情報と相手の公開情報から共有すべき暗号鍵を計算により求める方法。

<第3の方法>各エンティティの公開識別子を基にセンターが各エンティティの秘密アルゴリズムを作成し配送する準備をした後、通信相手の公開識別子と自分の秘密アルゴリズムから共有すべき暗号鍵を計算して求める方法。

【0003】

【発明が解決しようとする課題】

【表2】

<第1の方法の問題>第1の方法では、想定される通信相手の数が多いと管理に多大な手間を要し、不特定多数との暗号通信には不向きである。

<第2の方法の問題>第2の方法では、全エンティティが共通の鍵を共有することはできない。また、安全のため公開情報を変える場合、自分の秘密情報も変える必要があり管理しにくい。

<第3の方法の問題>第3の方法では、事前準備として各エンティティへ秘密アルゴリズムを配送する必要があるが、機密をたもったまま配送するためにはさらに他の機密管理機構が必要となる。また、全エンティティが共通の鍵を共有することは出来ない。更に、安全のため、自分の秘密アルゴリズムを変える場合、公開識別子を変える必要があり運用面での実用上、秘密アルゴリズムの再変更は困難である。

【0004】したがって、本発明は想定される通信相手の数が多くても管理に多大な手間を要することがなく、不特定多数との暗号通信に適していて、全エンティティが共通の鍵を共有することが可能で、また、安全のため公開情報を変える場合、自分の秘密情報を変更する必要がなく、管理が容易で、かつ事前準備として各エンティティへ秘密アルゴリズムを配送する必要がなく、機密を保ったまま配送するために、さらに他の機密管理機構を必要とせず、安全のため、自分の秘密アルゴリズムを変える目的で、公開識別子を変えるなどの実用上困難な処理が必要ない共有暗号鍵による通信システム、同システム用サーバ装置、同システム用クライアント装置、及び通信システムにおける暗号鍵の共有方法を提供することを目的とする。

【0005】

【課題を解決するための手段】本発明は上記目的を達成するために、従来のセンター管理暗号鍵共有方法では、共有する暗号鍵を変えるためにはクライアント側の暗証番号を変える必要があったのに対して、クライアント側の暗証番号は一定のまま、サーバの制御変数の変更のみで共有する暗号鍵を変更できるようにしている。このため、短い時間間隔で、共有する暗号鍵を変化させるシステム運用が可能となり、暗号システムの安全性が飛躍的に向上する。また、従来のセンター管理暗号鍵共有方法では、同じグループに属するすべてのクライアントで同じ暗号鍵を共有することはできなかったのに対して、サーバの制御変数がある特定の値に設定することでサーバ所属のクライアントグループ内で同じ暗号鍵を共有できるようにしている。このため、緊急時など、特別な状況においてサーバの制御のみでグループ内の暗号化を解除することができる。

【0006】すなわち本発明によれば、少なくともクライアントA、クライアントB、サーバS1により構成される共有暗号鍵による通信システムであって、前記クライアントAは、予め定めた自分の暗証番号a及び固有id生成アルゴリズム[I]、並びに暗号鍵生成アルゴリズム[K]を保持する記憶手段と、前記暗証番号a及び固有id生成アルゴリズム[I]を用いて固有id I(a)を生成する手段と、生成された固有id I(a)を前記サーバS1へ通知する手段と、前記クライアントBとの共通鍵を生成するために、前記サーバS1へ前記クライアントBの公開idを要求する手段と、前記サーバS1から送信される前記クライアントBの公開id S(I(b), v1)と前記暗証番号aを入力として前記暗号鍵生成アルゴリズム[K]を用いて暗号鍵 $K(S(I(b), v1), a)$ を生成する手段とを有し、前記クライアントBは、予め定めた自分の暗証番号b及び固有id生成アルゴリズム[I]、並びに暗号鍵生成アルゴリズム[K]を保持する記憶手段と、前記暗証番号b及び固有id生成アルゴリズム[I]を用い

て固有  $id\ I(b)$  を生成する手段と、生成された固有  $id\ I(b)$  を前記サーバ  $S1$  へ通知する手段と、前記サーバ  $S1$  又は前記クライアント  $A$  及びクライアント  $B$  が接続されたネットワーク経由で前記クライアント  $A$  の公開  $id$  を入手し、前記クライアント  $A$  の公開  $id\ S(I(a), v1)$  と前記暗証番号  $b$  を入力として前記暗号鍵生成アルゴリズム  $[K]$  を用いて暗号鍵  $K(S(I(a), v1), b)$  を生成する手段とを有し、前記サーバ  $S1$  は制御変数  $v1$  を生成する手段と、前記クライアント  $A$  から通知された固有  $id\ I(a)$  及び前記クライアント  $B$  から通知された固有  $id\ I(b)$  を保持するとともに、秘密で管理する前記制御変数  $v1$  並びに公開  $id$  生成アルゴリズム  $[S]$  を保持する記憶手段と、前記クライアント  $A$  からの要求を受けたときは、前記クライアント  $B$  の固有  $id\ I(b)$  と前記制御変数  $v1$  と、前記公開  $id$  生成アルゴリズム  $[S]$  を用いて前記クライアント  $B$  の公開  $id\ S(I(b), v1)$  を生成する手段と、生成された前記クライアント  $B$  の公開  $id\ S(I(b), v1)$  を前記クライアント  $A$  に送信する手段と、前記クライアント  $A$  の固有  $id\ I(a)$  と前記制御変数  $v1$ 、前記公開  $id$  生成アルゴリズム  $[S]$  を用いて前記クライアント  $A$  の前記公開  $id\ S(I(a), v1)$  を生成する手段と、生成された前記公開  $id\ S(I(a), v1)$  を前記クライアント  $A$  に送信する手段とを有し、前記アルゴリズム  $[I]$ 、 $[S]$ 、 $[K]$  が  $K(S(I(b), v1), a) = K(S(I(a), v1), b)$  を満足するものである共有暗号鍵による通信システムが提供される。

【0007】さらに本発明によれば、請求項1記載の共有暗号鍵による通信システム用サーバ装置であって、制御変数  $v1$  を生成する手段と、前記クライアント  $A$  から通知された固有  $id\ I(a)$  及び前記クライアント  $B$  から通知された固有  $id\ I(b)$  を保持するとともに、秘密で管理する前記制御変数  $v1$  並びに公開  $id$  生成アルゴリズム  $[S]$  を保持する記憶手段と、前記クライアント  $A$  からの要求を受けたときは、前記クライアント  $B$  の固有  $id\ I(b)$  と前記制御変数  $v1$  と、前記公開  $id$  生成アルゴリズム  $[S]$  を用いて前記クライアント  $B$  の公開  $id\ S(I(b), v1)$  を生成する手段と、生成された前記クライアント  $B$  の公開  $id\ S(I(b), v1)$  を前記クライアント  $A$  に送信する手段と、前記クライアント  $A$  の固有  $id\ I(a)$  と前記制御変数  $v1$ 、前記公開  $id$  生成アルゴリズム  $[S]$  を用いて前記クライアント  $A$  の前記公開  $id\ S(I(a), v1)$  を生成する手段と、生成された前記公開  $id\ S(I(a), v1)$  を前記クライアント  $A$  に送信する手段とを有する共有暗号鍵による通信システム用サーバ装置が提供される。

【0008】さらに本発明によれば、請求項1記載の共

有暗号鍵による通信システム用クライアント装置であって、予め定めた自分の暗証番号  $a$  及び固有  $id$  生成アルゴリズム  $[I]$ 、並びに暗号鍵生成アルゴリズム  $[K]$  を保持する記憶手段と、前記暗証番号  $a$  及び固有  $id$  生成アルゴリズム  $[I]$  を用いて固有  $id\ I(a)$  を生成する手段と、生成された固有  $id\ I(a)$  を前記サーバ  $S1$  へ通知する手段と、前記クライアント  $B$  との共通鍵を生成するために、前記サーバ  $S1$  へ前記クライアント  $B$  の公開  $id$  を要求する手段と、前記サーバ  $S1$  から送信される前記クライアント  $B$  の公開  $id\ S(I(b), v1)$  と前記暗証番号  $a$  を入力として前記暗号鍵生成アルゴリズム  $[K]$  を用いて暗号鍵  $K(S(I(b), v1), a)$  を生成する手段とを有する共有暗号鍵による通信システム用クライアント装置が提供される。

【0009】さらに本発明によれば、少なくともクライアント  $A$ 、クライアント  $B$ 、サーバ  $S1$  により構成される通信システムにおける暗号鍵の共有方法であって、前記クライアント  $A$  が、前もって自分の暗証番号  $a$  を定め、固有  $id$  生成アルゴリズム  $[I]$  を用いて固有  $id\ I(a)$  を生成するステップと、生成された固有  $id\ I(a)$  を前記サーバ  $S1$  へ通知するステップと、前記クライアント  $B$  が、前もって自分の暗証番号  $b$  を定め、固有  $id$  生成アルゴリズム  $[I]$  を用いて固有  $id\ I(b)$  を生成するステップと、生成された固有  $id\ I(b)$  を前記サーバ  $S1$  へ通知するステップと、前記クライアント  $A$  が、前記クライアント  $B$  との共通鍵を生成するために、前記サーバ  $S1$  へ前記クライアント  $B$  の公開  $id$  を要求するステップと、前記サーバ  $S1$  が前記クライアント  $A$  からの要求を受け、保有している前記クライアント  $B$  の固有  $id\ I(b)$  と前記サーバ  $S1$  が秘密で管理している制御変数  $v1$  を入力として、公開  $id$  生成アルゴリズム  $[S]$  を用いて前記クライアント  $B$  の公開  $id\ S(I(b), v1)$  を生成するステップと、生成された前記クライアント  $B$  の公開  $id\ S(I(b), v1)$  を前記クライアント  $A$  に送信するステップと、前記サーバ  $S1$  が、保有している前記クライアント  $A$  の固有  $id\ I(a)$  と  $v1$  から前記クライアント  $A$  の公開  $id\ S(I(a), v1)$  を生成するステップと、生成された前記クライアント  $A$  の公開  $id\ S(I(a), v1)$  を前記クライアント  $A$  に送信するステップと、前記クライアント  $A$  が入手した前記クライアント  $B$  の公開  $id\ S(I(b), v1)$  と前記暗証番号  $a$  を入力として暗号鍵生成アルゴリズム  $[K]$  を用いて暗号鍵  $K(S(I(b), v1), a)$  を生成するステップと、前記クライアント  $B$  が前記サーバ  $S1$  又は前記クライアント  $A$  及び前記クライアント  $B$  の接続されたネットワーク経由で前記クライアント  $A$  の公開  $id$  を入手し、暗号鍵  $K(S(I(a), v1), b)$  を生成するステップとを有し、前記アルゴリズム  $[I]$ 、



[S]、[K]が $K(S(I(b), v1), a) = K(S(I(a), v1), b)$ を満足するものである共有暗号鍵による通信システムにおける暗号鍵の共有方法が提供される。

【0010】さらに本発明によれば、少なくともサーバS1に管理されるクライアントA、サーバS2に管理されるクライアントC、前記サーバS1と前記サーバS2を管理する親サーバS3により構成される共有暗号鍵による通信システムであって、前記クライアントAは、予め定めた自分の暗証番号a及び固有id生成アルゴリズム[I]、並びに暗号鍵生成アルゴリズム[K]を保持する記憶手段と、前記暗証番号a及び前記固有id生成アルゴリズム[I]を用いて固有id I(a)を生成する手段と、生成された固有id I(a)を前記サーバS1へ通知する手段と、前記クライアントCとの共通鍵を生成するために、前記サーバS1へ前記クライアントCの公開idを要求する手段と、前記サーバS1から送信される前記クライアントCの3次公開id S(S(S(I(c), v2), v3), v1)と前記暗証番号aを入力として前記暗号鍵生成アルゴリズム[K]を用いて暗号鍵  $K(S(S(S(I(c), v2), v3), v1), a)$  を生成する手段とを有し、前記クライアントCは、予め定めた自分の暗証番号c及び固有id生成アルゴリズム[I]、並びに暗号鍵生成アルゴリズム[K]を保持する記憶手段と、前記暗証番号c及び固有id生成アルゴリズム[I]を用いて固有id I(c)を生成する手段と、生成された固有id I(c)を前記サーバS2へ通知する手段と、前記クライアントA及びクライアントCが接続されたネットワーク経由で前記クライアントAの3次公開id S(S(S(I(a), v1), v3), v2)を入手し、前記クライアントAの前記3次公開id S(S(S(I(a), v1), v3), v2)と前記暗証番号cを入力として前記暗号鍵生成アルゴリズム[K]を用いて暗号鍵  $K(S(S(S(I(a), v1), v3), v2), c)$  を生成する手段とを有し、前記サーバS1は前記クライアントAから通知された固有id I(a)を保持するとともに、秘密で管理する制御変数v1並びに公開id生成アルゴリズム[S]を保持する記憶手段と、前記クライアントAからの要求を受けたときは、要求相手が自グループに属するか否かを判断する手段と、自グループに属さない要求相手のときは前記親サーバS3に前記クライアントAからの要求を転送する手段と、前記親サーバS3から受信した前記クライアントCの2次公開id S(S(I(c), v2), v3)と、前記制御変数v1と、前記公開id生成アルゴリズム[S]から前記3次公開id S(S(S(I(c), v2), v3), v1)を生成して前記クライアントAに送信する手段とを有し、前記サーバS2は前記クライアントCから通知された固有id I(c)を保持する

とともに、秘密で管理する制御変数v2並びに公開id生成アルゴリズム[S]を保持する記憶手段と、前記親サーバS3からの要求を受けたときは、前記クライアントCの固有id I(c)と前記制御変数v2と、前記公開id生成アルゴリズム[S]を用いて前記クライアントCの1次公開id S(I(c), v2)を生成する手段と、生成された前記クライアントCの1次公開id S(I(c), v2)を前記親サーバS3に送信する手段とを有し、前記親サーバS3は前記サーバS2から送信された前記クライアントCの1次公開id S(I(c), v2)を保持するとともに、秘密で管理する制御変数v3並びに公開id生成アルゴリズム[S]を保持する記憶手段と、前記サーバS1からの要求を前記サーバS2に転送する手段と、前記サーバS2から前記クライアントCの1次公開id S(I(c), v2)を受けたときは、前記制御変数v3と、前記公開id生成アルゴリズム[S]を用いて前記クライアントCの前記2次公開id S(S(I(c), v2), v3)を生成する手段と、生成された前記クライアントCの2次公開id S(S(I(c), v2), v3)を前記サーバS1に送信する手段とを有し、前記アルゴリズム[I]、[S]、[K]が $K(S(S(S(I(c), v2), v3), v1), a) = K(S(S(S(I(a), v1), v3), v2), c)$ を満足するものである共有暗号鍵による通信システムが提供される。

【0011】さらに本発明によれば、請求項5記載の共有暗号鍵による通信システム用サーバS1であって、前記クライアントAから通知された固有id I(a)を保持するとともに、秘密で管理する制御変数v1並びに公開id生成アルゴリズム[S]を保持する記憶手段と、前記クライアントAからの要求を受けたときは、要求相手が自グループに属するか否かを判断する手段と、自グループに属さない要求相手のときは前記親サーバS3に前記クライアントAからの要求を転送する手段と、前記親サーバS3から受信した前記クライアントCの2次公開id S(S(I(c), v2), v3)と、前記制御変数v1と、前記公開id生成アルゴリズム

[S]から前記3次公開id S(S(S(I(c), v2), v3), v1)を生成して前記クライアントAに送信する手段とを有する共有暗号鍵による通信システム用サーバ装置が提供される。

【0012】さらに本発明によれば、請求項5記載の共有暗号鍵による通信システム用親サーバS3であって、前記サーバS2から送信された前記クライアントCの1次公開id S(I(c), v2)を保持するとともに、秘密で管理する制御変数v3並びに公開id生成アルゴリズム[S]を保持する記憶手段と、前記サーバS1からの要求を前記サーバS2に転送する手段と、前記サーバS2から前記クライアントCの1次公開id S(I(c), v2)を受けたときは、前記制御変数v3

と、前記公開  $i d$  生成アルゴリズム [S] を用いて前記クライアント C の前記 2 次公開  $i d$   $S(S(I(c), v2), v3)$  を生成する手段と、生成された前記クライアント C の 2 次公開  $i d$   $S(S(I(c), v2), v3)$  を前記サーバ S1 に送信する手段とを有する共有暗号鍵による通信システム用サーバ装置が提供される。

【0013】さらに本発明によれば、請求項 5 共有暗号鍵による通信システム用クライアント装置であって、予め定めた自分の暗証番号  $a$  及び固有  $i d$  生成アルゴリズム [I]、並びに暗号鍵生成アルゴリズム [K] を保持する記憶手段と、前記暗証番号  $a$  及び固有  $i d$  生成アルゴリズム [I] を用いて固有  $i d$   $I(a)$  を生成する手段と、生成された固有  $i d$   $I(a)$  を前記サーバ S1 へ通知する手段と、前記クライアント C との共通鍵を生成するために、前記サーバ S1 へ前記クライアント C の公開  $i d$  を要求する手段と、前記サーバ S1 から送信される前記クライアント C の 3 次公開  $i d$   $S(S(S(I(c), v2), v3), v1)$  と前記暗証番号  $a$  を入力として前記暗号鍵生成アルゴリズム [K] を用いて暗号鍵  $K(S(S(S(I(c), v2), v3), v1), a)$  を生成する手段とを有する共有暗号鍵による通信システム用クライアント装置が提供される。

【0014】さらに本発明によれば、少なくともサーバ S1 に管理されるクライアント A、サーバ S2 に管理されるクライアント C、前記サーバ S1 と前記サーバ S2 を管理する親サーバ S3 により構成される通信システムにおける暗号鍵の共有方法であって、前記クライアント A が、前もって自分の暗証番号  $a$  を定め、固有  $i d$  生成アルゴリズム [I] を用いて固有  $i d$   $I(a)$  を生成するステップと、生成された固有  $i d$   $I(a)$  を前記サーバ S1 へ通知するステップと、前記クライアント C が、前もって自分の暗証番号  $c$  を定め、固有  $i d$  生成アルゴリズム [I] を用いて固有  $i d$   $I(c)$  を生成するステップと、生成された固有  $i d$   $I(c)$  を前記サーバ S2 へ通知するステップと、前記クライアント A が、前記クライアント C との共通鍵を生成するために、前記サーバ S1 へ前記クライアント C の公開  $i d$  を要求するステップと、要求された通信相手である前記クライアント C が自グループに属するか否かを前記サーバ S1 が判断するステップと、前記クライアント C が自グループに属さないときは、前記サーバ S1 が前記親サーバ S3 へ前記クライアント C の公開  $i d$  を要求するステップと、前記親サーバ S3 が、前記サーバ S1 から要求された前記クライアント C を管理するサーバ S2 へクライアント C の公開  $i d$  を要求するステップと、前記サーバ S2 が、保有している前記クライアント C の固有  $i d$   $I(c)$  と自らの制御変数  $v2$  を入力としてアルゴリズム [S] を用いて、前記クライアント C の 1 次公開  $i d$

$S(I(c), v2)$  を生成するステップと、前記サーバ S2 が、生成された前記 1 次公開  $i d$  を前記親サーバ S3 へ送信するステップと、前記親サーバ S3 が、前記 1 次公開  $i d$   $S(I(c), v2)$  と自らの制御変数  $v3$  を入力としてアルゴリズム [S] を用いて、2 次公開  $i d$   $S(S(I(c), v2), v3)$  を生成するステップと、前記親サーバ S3 が生成された前記 2 次公開  $i d$   $S(S(I(c), v2), v3)$  を前記サーバ S1 へ送信するステップと、前記サーバ S1 が前記 2 次公開  $i d$   $S(S(I(c), v2), v3)$  と前記制御変数  $v1$  と前記アルゴリズム [S] を用いて、3 次公開  $i d$   $S(S(S(I(c), v2), v3), v1)$  を生成するステップと、前記サーバ S1 が、生成された前記 3 次公開  $i d$   $S(S(S(I(c), v2), v3), v1)$  を前記クライアント A へ送信するステップと、前記クライアント A が前記 3 次公開  $i d$   $S(S(S(I(c), v2), v3), v1)$  と前記暗証番号  $a$  とアルゴリズム [K] を用いて暗号鍵  $K(S(S(S(I(c), v2), v3), v1), a)$  を生成するステップと、前記クライアント C が前記暗証番号  $c$  とアルゴリズム [K] を用いて暗号鍵  $K(S(S(I(a), v1), v3), v2), c)$  を生成するステップとを有し、前記アルゴリズム [I]、

[S]、[K] が  $K(S(S(S(I(c), v2), v3), v1), a) = K(S(S(S(I(a), v1), v3), v2), c)$  を満足するものである共有暗号鍵による通信システムにおける暗号鍵の共有方法が提供される。

#### 【0015】

【発明の実施の形態】以下、本発明の共有暗号鍵による通信システム、同システム用サーバ装置、同システム用クライアント装置、及び通信システムにおける暗号鍵の共有方法の実施の形態を好ましい実施例によって図面に従い詳細に説明する。図 1 は、本発明の共有暗号鍵による通信システムの一例を示すブロック図である。本発明の適用される暗号通信のネットワークは、2 つ以上のクライアントと 1 つ以上のサーバから構成されており、クライアントはいずれかのサーバに所属している。また、図 1 の例のようにサーバが複数ある場合、これらは論理的な階層構造でネットワーク化されており、下位のサーバはいずれかの上位サーバに所属する。下位サーバを収容する上位サーバを親サーバと呼び、同じ親サーバに所属する下位サーバとクライアント群をグループと呼ぶ。なお、クライアントにおけるソフトウェアを含んだハードウェアをクライアント装置といい、同様にサーバにおけるソフトウェアを含んだハードウェアをサーバ装置という。なお、本発明はサーバの数によって制限を受けるものではないが、一般的にはネットワークに分散配置された、公開  $i d$  を管理する複数のサーバを有するシステムに適用可能である。

【0016】サーバより共有暗号鍵を生成するためのサービスを受け、共有暗号鍵を生成した後、それを用いて暗号化通信を行う主体であるクライアントには、コンピュータ、ICカード、移動体通信機等、全ての通信・情報処理装置が該当する。また、クライアントに対し共有暗号鍵を生成するためのサービスを提供する主体であるサーバにはコンピュータ、移動体通信制御装置等、全ての通信・情報処理装置が該当する。なお、各クライアント、サーバはCPU（中央演算処理装置）、メモリ、インターフェース等を有し、所定の通信機能、データ保持機能を有しているものとする。なお、ネットワークを構成する通信回線は、公衆回線、高速デジタル回線などの有線のみならず、電波や光などを用いた無線通信も含まれ、有線と無線の組合わせも含まれる。

【0017】全てのクライアントは公開可能な暗号鍵生成アルゴリズム[K]と固有id生成アルゴリズム

[I]を共通に持つ。固有idとは、各クライアントが秘密で保有する暗証番号を入力としてアルゴリズム

[I]により生成される値で、クライアントにより生成され、サーバへ送信の後、サーバで管理される。なお、暗証番号は、必ずしも数字のみならず、文字を含むことができる。また、アルゴリズム[I]の非可逆性により、固有idから暗証番号への逆変換は困難である。全てのサーバは公開可能な公開id生成アルゴリズム

[S]を共通に持つ。公開idとは、クライアントの固有idとサーバの制御変数を入力としてアルゴリズム

[S]により生成される値で公開可能な値である。図2は、図1中のサーバS1と、これによって管理される複数のクライアント中の2つであるクライアントAとクライアントBがそれぞれ有する各アルゴリズムを模式的に示す図である。

【0018】次に暗号鍵の生成の手順について図2の例、すなわち同一のサーバS1に所属するクライアントA及びクライアントBが鍵を生成する場合を第1実施例として説明する。図3は第1実施例の模式図である。また、図4は図3の実施例におけるクライアントAのCPUの動作を説明するフローチャートであり、図5は図3の実施例におけるサーバS1のCPUの動作を説明するフローチャートである。

【0019】

【表3】

(1) クライアントAは、前もって自分の暗証番号aを定め、固有id生成アルゴリズム[I]を用いて固有id I(a)を生成し、サーバS1へ通知しておく。クライアントBも同様に固有id I(b)をサーバへ通知しておく。

(2) クライアントAは、クライアントBとの共通鍵を生成するために、サーバS1へクライアントBの公開idを要求する。

(3) サーバS1はクライアントAからの要求を受

け、保有しているクライアントBの固有id I(b)とサーバが秘密で管理している制御変数v1を入力として、公開id生成アルゴリズム[S]を用いてクライアントBの公開id S(I(b), v1)を生成しクライアントAに通知する。

(4) 同時に、サーバS1は、保有しているクライアントAの固有id I(a)とv1からクライアントAの公開id S(I(a), v1)を生成しクライアントAに通知する。

(5) クライアントAは入手したクライアントBの公開id S(I(b), v1)と自分の秘密の暗証番号aを入力として暗号鍵生成アルゴリズム[K]を用いて暗号鍵 K(S(I(b), v1), a)を生成する。

(6) クライアントBはサーバS1経由で又は、クライアントA及びクライアントBが接続されたネットワーク経由でクライアントAの公開idを入手し、暗号鍵 K(S(I(a), v1), b)を生成する。

【0020】次に上記方法で生成された暗号鍵を両クライアントA、Bで共有する手法について説明する。クライアントAとクライアントBで暗号鍵を共有するためには、 $K(S(I(b), v1), a) = K(S(I(a), v1), b) \cdots \text{式①}$ が成立する様なアルゴリズム[I]、[S]、[K]を用いればよい。

【0021】

【数1】この点について具体例を挙げて説明すると、例えば、pを素数、gをmod pにおける原始根として

$$[I]: I(x) = g^x \bmod p$$

$$[S]: S(x1, x2) = x1^{x2} \bmod p$$

$$[K]: K(x1, x2) = x1^{x2} \bmod p$$

とすると

$$K(S(I(b), v1), a)$$

$$= K(S(g^b \bmod p, v1), a)$$

$$= K((g^b \bmod p)^{v1} \bmod p, a)$$

$$= K((g^{b \cdot v1} \bmod p), a)$$

$$= (g^{b \cdot v1} \bmod p)^a \bmod p$$

$$= g^{b \cdot v1 \cdot a} \bmod p$$

【0022】

【数2】同様に

$$K(S(I(a), v1), b) = g^{a \cdot v1 \cdot b} \bmod p$$

となる。 $g^{b \cdot v1 \cdot a} \equiv g^{a \cdot v1 \cdot b} \pmod{p}$ であるから式①は成立し、クライアントAとクライアントBは暗号鍵を共有できる。

【0023】次に上記の手法で生成された暗号鍵により暗号化されたデータあるいは通信文を解読して平文化するために必要な暗号鍵の解除方法について説明する。ここではサーバS1に所属するクライアントA及びクライアントBが生成する共通鍵をサーバS1からの制御により特定の値とする方法について説明する。共通鍵を特定の値とすることは実質的に暗号化の解除を意味し、クライアント側の特別な手続き無しでサーバ側の制御のみで

可能であることが本方法の特徴である。先に説明した通り、クライアントAは共通鍵として $K(S(I(b), v1), a)$ を生成するが、 $a$ 及び $b$ は各々のクライアントのみが知る値でサーバが自由に制御できるのは制御変数 $v1$ のみである。

【0024】

【数3】したがって、 $a$ 及び $b$ の値のいかに関わらず $v1$ に対して特定の値を生み出すアルゴリズム[K]及び[S]を採用することで共通鍵を特定の値とすること

$$g^{b \cdot v1} \cdot a \equiv g^{b \cdot \psi(p)} \cdot a \equiv (g^b \cdot a)^{\psi(p)} \equiv 1 \pmod{p}$$

となり、特定の値1を持つ(記号" $\psi(p)$ "は" $\psi(p)$ 乗"を示す:以下同じ)。同様に、クライ

$$K(S(I(a), v1), b) = g^{a \cdot v1} \cdot b \equiv 1 \pmod{p}$$

となり、共通鍵を特定の値1に制御できる。

【0025】上記第1実施例の動作をクライアントAのクライアント装置に用いられるCPUの動作を示す図4のフローチャートとサーバS1のサーバ装置に用いられるCPUの動作を示す図5のフローチャートに沿って説明する。図4において、図示省略の所定のイニシャライズの後、ステップS10で通信要求の有無を検出し、要求があれば、ステップS11でサーバS1に接続する。いまクライアントAからクライアントBへの通信を行うものとし、ステップS12でサーバS1に対して通信相手であるクライアントBと自分(クライアントA)の公開idを要求する。ここでサーバS1は図5のステップS30、S31を経てクライアントAからの要求を読み込み、クライアントBとクライアントAの公開idをそれぞれ生成し(ステップS32、S33)、ステップS34でクライアントAに送信する。ステップS35は正常に送信が終了したか否かを判断するもので、正常でなければ、ステップS31から再度実行する。

【0026】図4のステップS13では、サーバS1から上記2つの公開idを受信したか否かを判断し、受信したときはサーバS1との通信を終了し(ステップS14)、次いで自分の暗証番号 $a$ を読み出して(ステップS15)、通信相手の公開idとアルゴリズム[K]を用いて暗号鍵を生成する(ステップS16)。次にクライアントBへ送信すべき通信文、すなわち電文を暗号鍵と所定の暗号化アルゴリズムに従って暗号化する(ステップS17)。暗号化が終了すると、通信相手又はネットワークに接続し、暗号文を送信する(ステップS18、S19、S20)。送信が正常に終了しないときはステップS21経由でステップS19、S20を再度実行する。なお、ネットワークに接続した場合は直接クライアントBに送信するのではなく、所定サーバのメモリに暗号文が保持され、クライアントBが、その後そのサーバにアクセスしてこれを取り出すこととなる。

【0027】次に異なるグループ間の鍵の共有方法について第2実施例として説明する。この第2実施例はサー

ができる。例えば、前述のアルゴリズム

$$[S]: S(x1, x2) = x1 \cdot x2 \pmod{p}$$

$$[K]: K(x1, x2) = x1 \cdot x2 \pmod{p}$$

の場合、

$$K(S(I(b), v1), a) = g^{b \cdot v1} \cdot a \pmod{p}$$

$$v1 = \psi(p) \quad (\psi(p): \text{オイラー函数})$$

を選択した場合、オイラーの定理により

ントBが生成する共通鍵も

バス1に属するクライアントAとサーバS2に属するクライアントCの鍵共有を説明する。なお、図6に示すようにサーバS1及びS2の親サーバをS3とする。また、クライアントAの固有id  $I(a)$ はサーバS1に、クライアントCの固有id  $I(c)$ はサーバS2に事前に通知されているものとする。

【0028】

【表4】第2実施例における動作は次のようになる。

(1) クライアントAはサーバS1にクライアントCの公開idを要求する。

(2) サーバS1はクライアントCが自グループでないで親サーバS3へクライアントCの公開idを要求する。

(3) 親サーバS3は、クライアントCを管理するサーバS2へクライアントCの公開idを要求する。なお、クライアントCを管理するサーバがS2であることはクライアント名の名付けに例えば、C-S2-S3の様な論理的な階層構造を表す方法を採用することで容易に実現できる。

(4) サーバS2は、保有しているクライアントCの固有id  $I(c)$ と自らの制御変数 $v2$ を入力としてアルゴリズム[S]を用いて、 $S(I(c), v2)$ を生成し、親サーバS3へ通知する。

(5) 親サーバS3は、 $S(I(c), v2)$ と自らの制御変数 $v3$ を入力としてアルゴリズム[S]を用いて、 $S(S(I(c), v2), v3)$ を生成し、サーバS1へ通知する。

(6) サーバS1も同様に、 $S(S(S(I(c), v2), v3), v1)$ を生成し、クライアントAへ通知する。

(7) クライアントAはアルゴリズム[K]を用いて暗号鍵 $K(S(S(S(I(c), v2), v3), v1), a)$ を生成する。

(8) クライアントCも同様に、暗号鍵 $K(S(S(S(I(a), v1), v3), v2), c)$ を生成する。

【0029】

【数4】 前述のアルゴリズム

$$[I] : I(x) = g^x \bmod p$$

$$\begin{aligned} & K(S(S(S(I(c), v2), v3), v1), a) \\ &= K(S(S(S(g^c \bmod p), v2), v3), v1), a) \\ &= K(S(S(g^c \cdot v2 \bmod p), v3), v1), a) \\ &= K(S(g^c \cdot v2 \cdot v3 \bmod p), v1), a) \\ &= K(g^c \cdot v2 \cdot v3 \cdot v1 \bmod p), a) \\ &= g^c \cdot v2 \cdot v3 \cdot v1 \cdot a \bmod p \end{aligned}$$

また、同様に

$$\begin{aligned} & K(S(S(S(I(a), v1), v3), v2), c) \\ &= g^a \cdot v1 \cdot v3 \cdot v2 \cdot c \bmod p \\ & g^c \cdot v2 \cdot v3 \cdot v1 \cdot a \equiv g^a \cdot v1 \cdot v3 \cdot v2 \cdot c \pmod{p} \end{aligned}$$

であるからグループの異なるクライアント間でも暗号鍵を共有できることがわかる。

【0030】 上記各実施例では、2つのクライアント間の通信について説明したが、クライアント数が増加しても、同様の原理で暗号の共有化を図ることができる。また、ネットワークが図1に示した構成よりさらに複雑化して、サーバが3段以上の階層に配された場合でも同様に暗号の共有化を図ることができる。

【0031】

【発明の効果】 本発明の共有暗号鍵による通信システム、同システム用サーバ装置、同システム用クライアント装置、及び通信システムにおける暗号鍵の共有方法は上記のように構成されているので、次のような効果を有する。すなわち、従来のセンター管理暗号鍵共有方法では、共有する暗号鍵を変えるためにはクライアント側の暗証番号を変える必要があったが、本方法ではクライアント側の暗証番号は一定のまま、サーバの制御変数の変更のみで共有する暗号鍵を変更できる。このため、短い時間間隔で、共有する暗号鍵を変化させるシステム運用が可能となり、暗号システムの安全性が飛躍的に向上する。また、従来のセンター管理暗号鍵共有方法では、同じグループに属するすべてのクライアントで同じ暗号鍵を共有することはできなかったが、本方法ではサーバの制御変数ある特定の値に設定することでサーバ所属のクライアントグループ内で同じ暗号鍵を共有できる。こ

$$[S] : S(x1, x2) = x1^{x2} \bmod p$$

$$[K] : K(x1, x2) = x1^{x2} \bmod p$$

の場合、

のため、緊急時など、特別な状況においてサーバの制御のみでグループ内の暗号化を解除することができる。

【図面の簡単な説明】

【図1】 本発明の共有暗号鍵による通信システムの適用される通信ネットワーク例を模式的に示すブロック図である。

【図2】 図1中のサーバS1と、これによって管理される複数のクライアント中の2つであるクライアントAとクライアントBがそれぞれ有する各アルゴリズムを模式的に示す図であり、本実施例の第1実施例に対応する図である。

【図3】 本発明の第1実施例における動作を模式的に示す図である。

【図4】 本発明の第1実施例におけるクライアントのCPUの動作を模式的に示すフローチャートである。

【図5】 本発明の第1実施例におけるサーバのCPUの動作を模式的に示すフローチャートである。

【図6】 本発明の第2実施例における動作を模式的に示す図である。

【図7】 従来の暗号鍵共有方法の1つを示す模式図である。

【図8】 従来の暗号鍵共有方法の1つを示す模式図である。

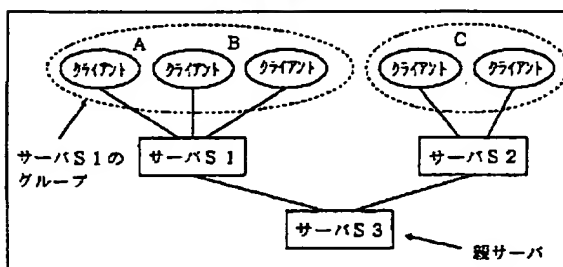
【図9】 従来の暗号鍵共有方法の1つを示す模式図である。

【符号の説明】

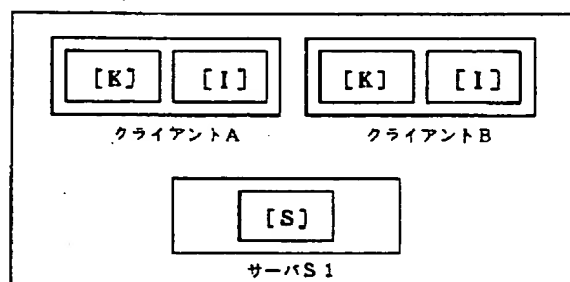
A、B、C クライアント装置

S1、S2、S3 サーバ装置

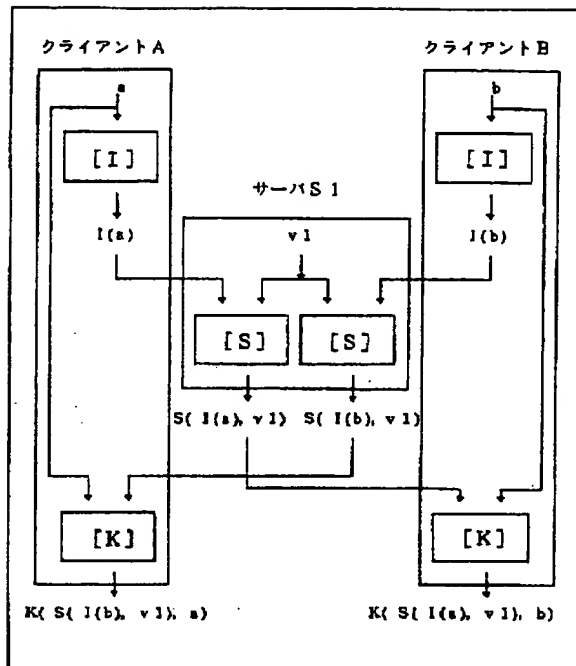
【図1】



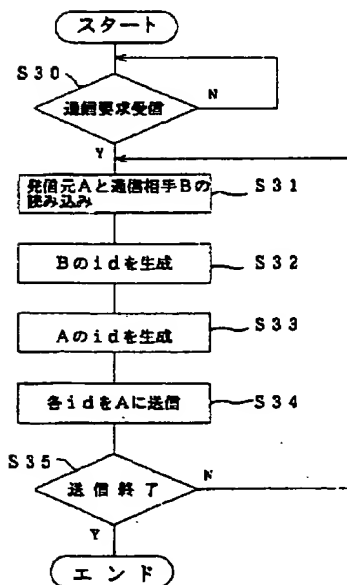
【図2】



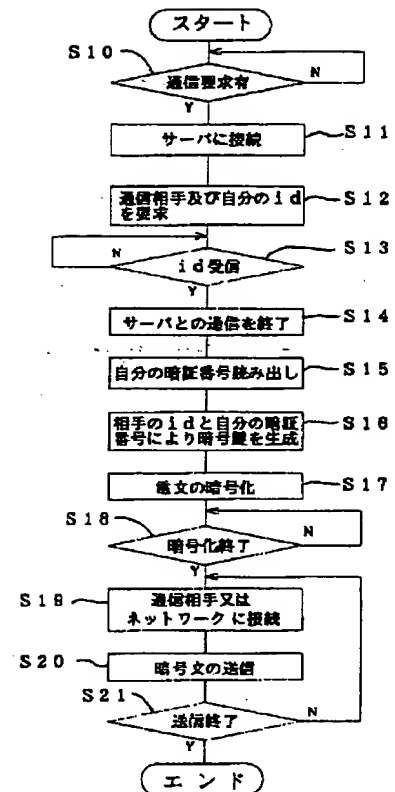
【図 3】



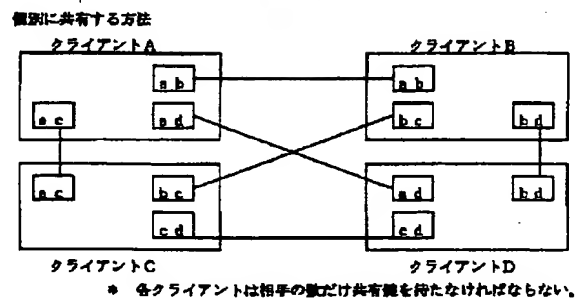
【図 5】



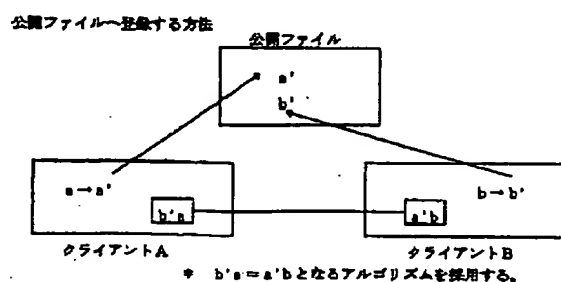
【図 4】



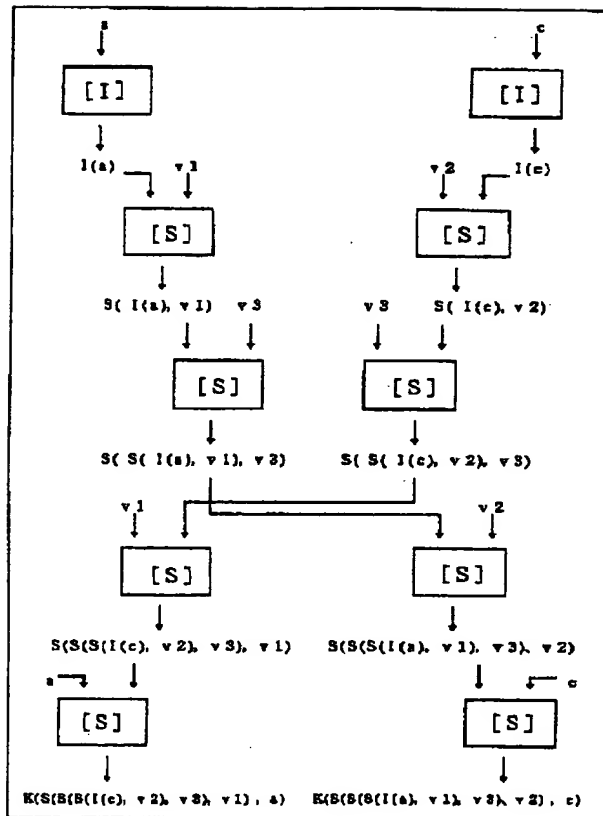
【図 7】



【図 8】



【図 6】



【図 9】

センターが事前配布する方法

